U.S. Nuclear Regulatory Commission Public Meeting Summary

Title: Draft Proposed Rule Text for Fuel Cycle Cyber Security

Meeting Identifier: 20160607

Date of Meeting: Thursday, May 19, 2016

Location: NRC Complex, NRC Three White Flint North, 11601 Landsdown Street, HQ-3WFN-1C03, Rockville MD

Type of Meeting: Category 3

Purpose of the Meeting(s): The purpose of the meeting was to provide stakeholders an early version of the draft proposed rule text for cyber security and to receive stakeholder feedback on the draft proposed rule text.

General Details:

The NRC staff conducted a public meeting/webinar beginning at 1:00 p.m. eastern standard time (EST) until approximately 4:00 p.m. On the day of the meeting, there was a loss of power to the NRC data center that resulted in internet and telephone outages, which presented some difficult challenges to the public meeting. However, NRC staff overcame these extraordinary circumstances to ensure that the webinar, teleconference, and slide presentation for the meeting remained seamlessly integrated. The meeting was very successful for the staff and stakeholders. It provided stakeholder an opportunity to review and comment on the proposed rule text and allowed the staff to receive valuable feedback that will be used in further development of the draft proposed rule language.

There were at least 51 attendees at the meeting; 31 signed in remotely on the webinar/webcast with some locations having multiple attendees and 20 physically located in the room. The attendees included: industry stakeholders (32), NRC staff (18), and one member of the public (. A complete list of the attendees and the organizations represented is attached.

The summary below provides an overview of the meeting discussions. It is not a comprehensive or detailed record of all of the points made during the meeting. Additionally, it does not represent any NRC policy or decisions on the issues presented.

Summary of Presentations:

The U.S. Nuclear Regulatory Commission (NRC) is initiating a rulemaking to establish new cyber security regulations in Part 73 of Title 10 of the *Code of Federal Regulations* (10 CFR), "Physical Protection of Plants and Materials." The section proposed is 73.56, "Requirements for cyber security at nuclear fuel cycle facilities." The objective of this rulemaking is to develop and issue new regulatory requirements for nuclear fuel cycle facility (FCF) licensees. FCF licensees include those licensed under: (1) 10 CFR Part 70 and authorized to possess or use a formula quantity of strategic special nuclear material (SSNM) as defined in 10 CFR 73.2 (Category I

facilities); (2) 10 CFR Part 70 and authorized to possess or use special nuclear material (SNM) of moderate strategic significance as defined in 10 CFR 73.2 (Category II facilities); (3) 10 CFR Part 70 and authorized to possess or use SNM of low strategic significance as defined in 10 CFR 73.2 (Category III facilities); and (4) 10 CFR Part 40 and authorized to operate as conversion/deconversion.

The meeting presentation included the following: a status update and schedule discussion, an in-depth discussion on the draft proposed rule text, and a discussion of topics for the upcoming July and August 2016 public meeting. A copy of the PowerPoint presentations made at the meeting is available are available at: ADAMS Accession Number: ML16139A046.

Status Update and Timeline: The NRC staff provided an update on the proposed rulemaking timeline. The points highlighted included completion of the regulatory basis in March 2016. The final regulatory basis for the rulemaking was completed on March 2016 and was publically noticed in the Federal Register (81 FR 21449). As a result of the completion of the regulatory basis, the staff is now in the proposed rule phase of the rulemaking process and the NMSS rulemaking staff has assumed lead of this aspect of the project. In accordance with the Cumulative Effects of Regulation initiatives, staff indicated that they would appreciate any input from industry in the development of the Regulatory Analysis for the rulemaking. The fuel cycle industry indicated that they is willing to provide cost feedback and indicated that the staff should review he cost analysis from the cyber security for reactors rulemaking.

The NRC staff is considering additional opportunities for public input on the draft proposed rule and associated guidance prior to submission to the Commission. The next opportunity for public interaction is scheduled for July and August 2016.

In-Depth Discussion of Draft Proposed Rule Text:

Generic Comment: Many of the stakeholders indicated that the proposed rule text is too prescriptive. They recommended that much of the language in the draft proposed rule language should be moved to the guidance.

Applicability: Stakeholders indicated that the example timeframe to submit cyber security plan (CSP) as a license amendment request should be changed from the proposed 5 months after the final rule is effective to 6 months to align with the reactor cyber security rule. Stakeholder suggested that the NRC clarify how the CSP would be tied down in license, and how updates to the CSP would be implemented. In addition, stakeholders indicated that the NRC should consider making the format, submittal, and maintenance of the CSP consistent with requirements for similar plans required by the NRC‘s regulations.

Cyber security program performance objectives: Stakeholders indicated that that the term vital is used elsewhere in Part 73. They questioned whether it meant the same as that used in § 73.54. They further indicated that the term, “vital,” should be clearly defined to avoid confusion. It was also suggested that the NRC consider using another term, e.g., critical or some other phrase. Stakeholders indicated that much of the rule in this section appeared to be too prescriptive, and should be moved to the guidance document. In addition, stakeholders indicated that the draft proposed rule text is unclear on how to implement the performance

objectives of protect, detect, respond and recover and clarification is needed. It was also noted that this language is inconsistent with the proposed paragraph (b) which states licensees "shall establish, implement, and maintain a cyber security program." Stakeholders indicated that staff should consider language consistent with existing 73.54(c).

Consequences of concern: Stakeholders indicated that clarification is needed relative to the four types of consequences of concern – Active - safety (applies to all facilities, Latent - safety and security (applies to all facilities), Latent - safeguards (applies to Category II facilities), and Latent - design basis threat (applies to Category I facilities). Specifically, stakeholders indicated that staff should; (1) describe the protection of assets for active versus latent, and the distinction between the two, (2) since all consequences of concern are not equal, clarify how to grade controls, (3) clarify whether the cyber security controls are only determined by the consequences of concern, (4) consider using the phrase "technically feasible" for grading controls, and (5) clarify whether support systems only apply to active consequences of concern.

Cyber security program: Commenters indicated that staff should: (1) clarify what constitutes a support system, (2) clarify what the NRC meant by support systems must have a direct nexus to consequences of concern, (3) clarify that systems part of a classified network (U.S. Department of Energy [DOE] – Oak Ridge or National Nuclear Security Administration) are excluded from analysis (4) consider that some unclassified digital systems regulated by other agencies should be excluded from regulation by the NRC, and (5) clarify that systems with alternate means applied are adequately protected. Stakeholders also indicated that the proposed draft rule language in d(4)(i-ii) needs further clarification and should be more performance based. In addition, relative to draft proposed paragraph (d)(5), commenters indicated that the NRC staff should: (1) define what validation testing of digital assets mean, e.g., does the NRC mean that licensees need to validate controls, (2) consider making validation testing consistent with that of the NIST guidance, (3) clarify the frequency at which the validation needs to occur, and (4) clarify the type of testing required as part of validation. Furthermore, stakeholders suggested that NRC: (1) clarify what role interim compensatory measures play in maintenance and (2) consider moving interim compensatory measures to guidance.

Cyber security plan: Stakeholder indicated that the proposed draft rule text should be revised to clarify: (1) the number of cyber security plans required and (2) whether multiple plans will be required per site. The commenters also indicated that the section is too prescriptive and some of the information would be better suited for guidance. Stakeholders also questioned what the level of security for cyber security related documents should be. It was also recommended that a template be included in the guidance document.

Configuration management. No comments were received on this draft proposed language.

Biennial review of the cyber security program: The stakeholders had a number of comments regarding this draft proposed rule text. Commenters indicated that the section is too prescriptive and that information after the first sentence should be moved to the guidance. They also indicated that staff should clarify the following: (1) would licensees be required to do a review or a reaccreditation, and (2) is a 2 year reaccreditation envisioned? Commenters indicated that the NRC should not require a reaccreditation and should allow 3 year for the cyber security review. In addition, the stakeholders indicated that the NRC should consider

implementing a rolling cycle to allow a percentage of the controls to be reevaluated every year. They also indicated that the draft proposed section seems overly burdensome and that the section should be modified to clarify that the biennial review is focused on “verification” of the program. Furthermore, the commenters indicated that NRC should model the biennial review on the existing requirements after the 10 CFR 74 requirements for fundamental nuclear material control plans. In addition, commenters noted that the DOE compliant networks are required to do a full reaccreditation every year and the NRC should clarify how this program would demonstrate compliance with NRC regulations.

Event reporting and tracking: Some commenters indicated the draft proposed event reporting and tracking section needs clarification, including whether the reporting requirement is a log file or a reportable event and clarify what type of vulnerabilities need to be documented. Stakeholders also suggested that the staff consider using language similar to that in Appendix G of Part 73. Additionally, commenters also requested that response requirements for events allow the licensee maximum flexibility to respond to the event.

Records: Commenters indicated that staff should explain what is meant by the draft proposed language “retain all supporting technical documentation.” They elaborated that the draft proposed text could be overly burdensome for licensees and has the potential for including numerous documents.

Next Public Meetings: Staff will coordinate potential dates with stakeholders as soon as possible. Commenters indicated that staff should consider holding a workshop type meeting with industry to discuss the technical details of the cyber security controls. It was also suggested that staff consider holding a workshop prior to submitting the concurrence package so the industry comments can be incorporated.

Action Items/Next Steps:

The NRC staff plans to review the comments received during the public meeting and revise the draft proposed rule text. The revised draft proposed rule text and guidance will be discussed during public meetings to be held in July and August 2016.

Attachments:
Meeting agenda – ADAMS Accession No. ML16139A908
NRC staff presentation – ADAMS Accession No. ML16139A046
List of Attendees – Attached

List of Attendees
May 19, 2016, Public Meeting on the
Draft Proposed Rule Text for the Cyber Security for Fuel Cycle Facilities Rulemaking

	Last Name	First Name	Organization
1	Ani	Suzanne	NRC/NMSS
2	Antonescu	Christina	NRC/ACRS
3	Ashkeboussi	Nima	Nuclear Energy Institute
4	Bartelme	Jeffrey	Shine Medical
5	Bartlett	Matthew	NRC/NMSS
6	Beardsley	Jim	NRC/NSIR
7	Bergemann	Brad	NRC/NSIR
8	Bergman	Jana	Curtiss-Wright Nuclear
9	Clefton	Gordon	NRC/NMSS
10	Corrado	Jonathan	Centrus Energy Corp.
11	Costedio	Jim	Shine Medical
12	Deucher	Joe	NRC/NMSS
13	Dolley	Steven	SP Global
14	Downs	James	NRC/NMSS
15	Fishel	Bryan	General Electric
16	Freepons	Linda	AREVA
17	Gomez	Antonio	NRC/NRR
18	Grundman	Dan	DG Performance Services
19	Haeger	Allan	Certrec Corp.
20	Hamby	Gary	Honeywell
21	Hardin	Amy	NRC/OIG
22	Hawley	Jennifer	BWX Technologies
23	Jehle	Patty	NRC/OGC
24	Johns	William	NRC/NSIR
25	Lee	Dave	EMP Inc.
26	Lewis	Marvin	Public
27	Link	Robert	Nuclear Energy Institute
28	Maltese	Jim	NRC/OGC
29	Martin	Tony	BWX Technologies
30	Mattox	Bruce	General Electric
31	Maupin	Cardelia	NRC/NMSS
32	Maxwell	Brandon	URENCO
33	McGowen	Bryan	URENCO
34	Monks	Mark	General Electric
35	Murray	Scott	General Electric
36	Neas	Brent	BWX Technologies
37	Parr	Nancy	Westinghouse
38	Pantalo	Charity	NRC/NSIR
39	Rander	Andrew	BWX Technologies
40	Reeves	James	Global Nuclear Fuels
41	Rund	Jonathan	Nuclear Energy Institute
42	Schlueter	Janet	Nuclear Energy Institute
43	St Amour	Norm	NRC/OGC
44	Stewart	Danny	Global Nuclear Fuels
45	Sturzebecher	Karl	NRC/NMSS
46	Teyssier	David	AREVA
47	Vinson	Ken	Shine Medical

48	Walley	John	NRC/NSIR
49	Williams	Drew	General Electric
50	Wuokko	Dale	Global Energy
51	Zozula	Camille	Westinghouse